

In re Application of: Shelest et al.
Serial Number: 10/010,352

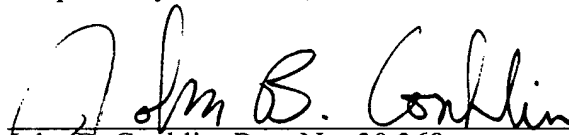
REMARKS

Claims 1 through 22 are pending. No claims currently stand allowed. The proposed amendments to claims 2, 5, 8, 10, 17, and 20 raise these dependent Beauregard claims to independent status. The proposed amendment to claim 21 is intended to more particularly point out and more distinctly claim the invention. No new matter has been added.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,



John B. Conklin, Reg. No. 30,369
One of the Attorneys for Applicants
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: March 25, 2002

APPENDIX A
Marked-Up Copy of Amendments to the Claims

2. (Amended) A computer-readable medium containing instructions for performing [the] a method [of claim 1] for a first computing device to make authentication information available to a second computing device, the method comprising:
creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and
making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the digital signature in a packet option.

5. (Amended) A computer-readable medium containing instructions for performing [the] a method [of claim 3] for a second computing device to authenticate content data made available by a first computing device, the method comprising:
accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;
deriving a portion of a second network address from the public key of the first computing device;
validating the digital signature by using the public key of the first computing device;
and
accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data,
wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded.

8. (Amended) A computer-readable medium containing instructions for performing [the] a method [of claim 6] for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the method comprising:
 - hashing the public key;
 - comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion;
 - if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing; and
 - if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing.
10. (Amended) A computer-readable medium containing instructions for performing [the] a method [of claim 9] for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device, the method comprising:
 - hashing the public key and at least a portion of the route prefix of the network address;
 - setting the node-selectable portion of the network address to a portion of the value produced by the hashing;
 - checking to see if the network address as set is already in use; and
 - if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking.
17. (Amended) A computer-readable medium containing instructions for performing [the] a method [of claim 11] for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:
 - accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;
 - deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device;
and

caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data.

20. (Amended) A computer-readable medium containing instructions for performing [the] a method [of claim 18] for a computing device to use a cache of at least one public key/network address association, the method comprising:

accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, and a network address of the first computing device;

comparing the public key and network address of the first computing device with a public key/network address association in the cache; and

accepting the content data if the public key and network address of the first network device match the public key/network address association in the cache.

21. (Amended) A computer-readable medium having stored thereon a data structure of authentication information, the data structure comprising:

a first data field containing data representing a public key of a computing device;
and

a second data field containing data representing a network address of the computing device, the network address derived, at least in part, from a hash of the public key.

APPENDIX B
Clean Copy of the Entire Set of Pending Claims

1. A method for a first computing device to make authentication information available to a second computing device, the method comprising:
creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and
making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the digital signature in a packet option.
2. A computer-readable medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device, the method comprising:
creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and
making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the digital signature in a packet option.

In re Application of: Shelest et al.
Serial Number: 10/010,352

3. A method for a second computing device to authenticate content data made available by a first computing device, the method comprising:
 - accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;
 - deriving a portion of a second network address from the public key of the first computing device;
 - validating the digital signature by using the public key of the first computing device; and
 - accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data,
 - wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded.
4. The method of claim 3 wherein the second computing device accesses the public key of the first computing device over an insecure channel to a device in the set: the first computing device, a key publishing device.

5. A computer-readable medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device, the method comprising:
 - accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;
 - deriving a portion of a second network address from the public key of the first computing device;
 - validating the digital signature by using the public key of the first computing device;
 - and
 - accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data,
 - wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded.
6. A method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the method comprising:
 - hashing the public key;
 - comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion;
 - if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing; and
 - if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing.
7. The method of claim 6 wherein the portion of the network address other than the node-selectable portion comprises an element in the set: "u" bit, "g" bit, a portion of a route prefix.

8. A computer-readable medium containing instructions for performing a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the method comprising:
 - hashing the public key;
 - comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion;
 - if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing; and
 - if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing.
9. A method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device, the method comprising:
 - hashing the public key and at least a portion of the route prefix of the network address;
 - setting the node-selectable portion of the network address to a portion of the value produced by the hashing;
 - checking to see if the network address as set is already in use; and
 - if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking.
10. A computer-readable medium containing instructions for performing a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device, the method comprising:
 - hashing the public key and at least a portion of the route prefix of the network address;
 - setting the node-selectable portion of the network address to a portion of the value produced by the hashing;
 - checking to see if the network address as set is already in use; and
 - if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking.

11. A method for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:
 - accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;
 - deriving a portion of a second network address from the public key of the first computing device;
 - validating the digital signature by using the public key of the first computing device; and
 - caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data.
12. The method of claim 11, wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address.
13. The method of claim 11, further comprising:
 - determining whether to cache the public key in association with the first network address based on a time stamp in the authentication information.
14. The method of claim 11 further comprising:
 - comparing the first network address against a network address in a public key/network address association already in the cache; and
 - if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then discarding the public key and first network address without caching them.

15. The method of claim 14 further comprising:
 - if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then removing from the cache the public key/network address association already in the cache.
16. The method of claim 11 further comprising:
 - associating a timer with the caching of the public key/network address association;
 - resetting the timer if a second public key/network address association, identical to the public key/network address association, is presented for caching; and
 - if the timer expires, removing the public key/network address association from the cache.
17. A computer-readable medium containing instructions for performing a method for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:
 - accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;
 - deriving a portion of a second network address from the public key of the first computing device;
 - validating the digital signature by using the public key of the first computing device;
 - and
 - caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data.

18. A method for a computing device to use a cache of at least one public key/network address association, the method comprising:
 - accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, and a network address of the first computing device;
 - comparing the public key and network address of the first computing device with a public key/network address association in the cache; and
 - accepting the content data if the public key and network address of the first network device match the public key/network address association in the cache.
19. The method of claim 18, further comprising:
 - determining whether to accept the content data based on a time stamp in the authentication information.
20. A computer-readable medium containing instructions for performing a method for a computing device to use a cache of at least one public key/network address association, the method comprising:
 - accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, and a network address of the first computing device;
 - comparing the public key and network address of the first computing device with a public key/network address association in the cache; and
 - accepting the content data if the public key and network address of the first network device match the public key/network address association in the cache.
21. A computer-readable medium having stored thereon a data structure of authentication information, the data structure comprising:
 - a first data field containing data representing a public key of a computing device; and
 - a second data field containing data representing a network address of the computing device, the network address derived, at least in part, from a hash of the public key.

In re Application of: Shelest et al.
Serial Number: 10/010,352

22. The data structure of claim 21 further comprising:
a third data field containing data representing a time stamp.